



# Department of Energy

# Insider Threat Program



Department of Energy  
2023 Energy Facility Contractors Group (EFCOG)  
Safeguards & Security Working Group

Sabeena Khanna  
Director  
Office of Insider Threat Program (EHSS-1.21)  
May 3, 2023

Discovery Hall, 650 Horn Rapids Road,  
Pacific Northwest National Laboratory, Richland, WA





# The Policies Behind the Program



**\*\*\*Goal is to begin revision of DOE Order 470.5 (via the DRB process) in Calendar Year (CY) 2023\*\*\***

## National Policy

***Executive Order 13587,***  
*“Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information” (October 7, 2011)*

***National Insider Threat Policy and Minimum Standards***  
*(November 21, 2012)*

## DOE Policy

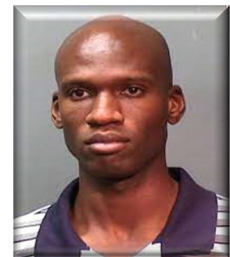
***DOE Order 470.5,***  
*“Insider Threat Program”*  
*(June 2, 2014)*



# History of the Program

## The Impetus: The Three Incidents

- **2010 WikiLeaks**. U.S. Army intelligence analyst Pvt. Manning delivered hundreds of thousands of classified documents that he found troubling to WikiLeaks and was sentenced for espionage and theft.
- **2013 Classified Document Cache Leak**. Edward Snowden leaked vast amounts of classified information that did untold damage to U.S. national security as well as the national security of allied nations.
- **2013 Navy Yard Shootings**. Aaron Alexis fatally shot twelve people at the headquarters of the Naval Sea Systems Command (NAVSEA), Washington Navy Yard in southeast Washington, D.C. It was the second-deadliest mass shooting on a U.S. military base, behind the 2009 Fort Hood shooting.
- **2023**. The recent case of the Massachusetts Air National Guard Airman underscores the need for effective and robust Insider Threat Programs.





# Insider Threat Programs: The Beginning

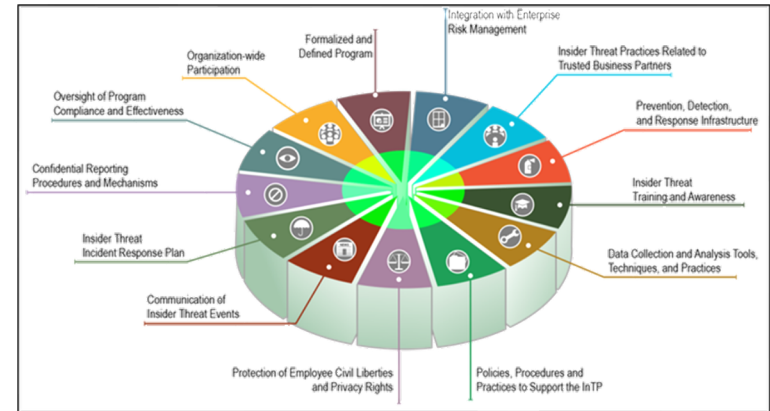
- United States Government (USG) Insider Threat Programs tended to focus exclusively on User Activity Monitoring (UAM) and the safeguarding of classified information from 2011 - ~2013.
- During this time period, the locus and ethos of USG Insider Threat Programs also tended to be intelligence and counterintelligence-centric; and housed within those elements.





# Where We Are Now

- The Insider Threat Program community has moved away from the intelligence / counterintelligence position and towards a more human behavior focus to look at a holistic approach to the insider threat problem set.
- The National Counterintelligence and Security Center (NCSC), home of the National Insider Threat Task Force (NITTF), on record stated that:



*“An insider threat program is not a security program;  
it is not a cybersecurity (information security) program;  
and it is not a counterintelligence program.  
It is a new and unique discipline focused on human behavior –  
looking for anomalies, contextualizing them, and facilitating an  
appropriate organization response...”*

- NCSC, “Insider Threat Mitigation for U.S. Critical Infrastructure Entities: Guidelines from an Intelligence Perspective,” March 2021.

**Office of Environment, Health, Safety and Security**



# The Mission: Going Forward

- Secretary Granholm's February 7<sup>th</sup> memo outlines clear direction on the way forward vis-à-vis the DOE Insider Threat Program.
  - Makes clear the Secretary's intent and vision per the Insider Threat Program.
  - Outlines and describes the role of the Designated Senior Official (DSO), the Office of Insider Threat Program (OITP), the Analysis and Referral Center (ARC) and the Local Insider Threat Working Groups (LITWGs).
  - Emphasizes the necessity for ongoing, close coordination with all DOE Program and Support Offices in order to achieve mission success.



# Immediate and Long Term Focus

- Developing a Near-Term Strategy Plan (NTSP)
- Drafting an Insider Threat Program Annual Report
- Drafting a Long-Term Strategy Plan (LTSP)
- Revising DOE Order 470.5
- Continuing to enhance the balancing of Privacy and Civil Liberties with the Insider Threat Program mission
- Increased incorporation of Behavioral Science and People-Risk disciplines



# Reporting Indicators

**Report indicators of insider threat to:**

- **Your Local LITWG**

Contact Information can be found on <https://itp.energy.gov>

- **Intelligence Operations Center (IOC)**

Phone: 202-586-3335 (unclassified insider threat-related matters)

- **ARC**

Email: [insiderthreat@doe.gov](mailto:insiderthreat@doe.gov) (unclassified)  
[insiderthreat@doe.ic.gov](mailto:insiderthreat@doe.ic.gov) (classified)





# Contact Information

Reach out to the **Office of Insider Threat Program** for more information (or if you have questions) specifically relating to Insider Threat Program policy/training.

**Office: (202) 586-9020**

**Email: [itpmo@hq.doe.gov](mailto:itpmo@hq.doe.gov)**

**Website: <https://itp.energy.gov>**

Reach out to the **Analysis and Referral Center** for more information (or if you have questions) relating to UAM/operations.

**Office: (202) 586-9099**

**Email: [insiderthreat@doe.gov](mailto:insiderthreat@doe.gov) (unclassified)**

**[insiderthreat@doe.ic.gov](mailto:insiderthreat@doe.ic.gov) (classified)**

***“Together, we’ve got it covered”***

**Office of Environment, Health, Safety and Security**